CLAIMS

What is claimed is:

1. A method for encryption and decryption of electronic messages based on an encryption protocol, the method comprising the computer-implemented steps of:

receiving a first electronic message that is encrypted according to the encryption protocol;

generating at least one part of a second electronic message, based on at least the first electronic message, a modular operation that is based on two applications of Montgomery's method, a first operand, a second operand, and a modulus, and wherein the step of generating the second electronic message includes the computer-implemented steps of:

generating a first constant based on the modulus;

determining an intermediate result based on at least Montgomery's method for the modular operation, the first operand, and the first constant; and

determining and storing in memory a final result that comprises the at least one part of the second electronic message, based on at least Montgomery's method for the modular operation, the intermediate result, and the second operand.

2. The method of Claim 1, wherein the encryption protocol is the Rivest-Shamir-Adleman public key protocol.

3. The method of Claim 1, wherein the encryption protocol is the Diffie-Hellman key agreement protocol.

4. The method of Claim 1, wherein the encryption protocol is the digital signature algorithm protocol.

5. The method of Claim 1, wherein the step of generating the first constant based on the modulus includes the computer-implemented steps of:

selecting a second constant that satisfies a specified relationship with respect to the modulus; and

determining the first constant based on the second constant and the modulus.

6. The method of Claim 1, wherein the step of generating the first constant (R) based on the modulus (M) includes the computer-implemented steps of:

selecting a second constant (W) such that $W \geq 4M$; and

determining the first constant (R) according to the expression $R = W^2 \pmod{M}$.

7. The method of Claim 6, wherein the second constant (W) is not a power of two.

8. The method of Claim 1, wherein the first operand is a first 1024-bit operand and the second operand is a second 1024-bit operand.

9. The method of Claim 1, wherein the modular operation is a modular multiplication that is based on at least the first operand, the first constant, a second constant, the modulus, and a negative multiplicative inverse of the modulus, and wherein the intermediate result is determined by the computer-implemented steps of:

determining a modified first operand based on the first operand and the first constant;

determining a modular reduction of the modified first operand based on the modified first operand, the negative multiplicative inverse of the modulus, and the second constant; and

determining the intermediate result based on the modified first operand, the modular reduction of the modified first operand, the modulus, and the second constant.

10. The method of Claim 1, wherein the modular operation is a modular multiplication that is based on at least the first operand (X), the first constant (R), a second constant (W), the modulus (M), and a negative multiplicative inverse of the modulus (M′), and wherein the intermediate result (S) is determined based on the following expressions:

$$Z = XR;$$

$$U = ZM'(\mathrm{mod}(W)); \text{ and}$$

$$S = (Z + UM)/W.$$

11. The method of Claim 1, wherein the modular operation is a modular multiplication that is based on at least the second operand, a second constant, the modulus, a negative multiplicative inverse of the modulus, and the intermediate result, and wherein the final result is determined by the computer-implemented steps of:

determining a modified second operand based on the second operand and the intermediate result;

determining a modular reduction of the modified second operand based on the modified second operand, the negative multiplicative inverse of the modulus, and the second constant; and

determining the final result based on the modified second operand, the modular reduction of the modified second operand, the modulus, and the second constant.

12. The method of Claim 1, wherein the modular operation is a modular multiplication that is based on at least the second operand (Y), a second constant (W), the modulus (M), a negative multiplicative inverse of the modulus (M′), and the intermediate result (S), and wherein the final result (F) is determined based on the following expressions:

$Z = YS;$

$U = ZM'(\mathrm{mod}(W))$; and

$F = (Z + UM)/W.$

13. The method of Claim 1, wherein the modular operation is a modular exponentiation that is based on at least the first operand, the first constant, a second constant, the modulus, and a negative multiplicative inverse of the modulus, and wherein the intermediate result is determined by the computer-implemented steps of:

determining a modified first operand based on the first operand and the intermediate result;

determining a modular reduction of the modified second operand based on the modified second operand, the negative multiplicative inverse of the modulus, and the second constant; and

determining the intermediate result based on the modified second operand, the modular reduction of the modified second operand, the modulus, and the second constant.

14. The method of Claim 1, wherein the modular operation is a modular exponentiation that is based on at least the first operand (X), the first constant (R), a second constant (W), the modulus (M), and a negative multiplicative inverse of the modulus (M′), and wherein the intermediate result (S) is determined based on the following expressions:

$Z = XR$;

$U = ZM'(\mathrm{mod}(W))$; and

$S = (Z + UM)/W$.

15. The method of Claim 1, wherein the modular operation is a modular exponentiation that is based on at least the second operand, a second constant, the modulus, a negative multiplicative inverse of the modulus, and the intermediate result, wherein the second operand includes a plurality of digits, and wherein the final result is determined by the computer-implemented steps of:

specifying a previous final result as having a value of one and a previous intermediate result as the intermediate result;

for each digit of the plurality of digits included in the second operand, performing the computer-implemented steps of:

when each digit of the plurality of digits has the value of one, then performing the computer-implemented steps of:

determining an updated final result based on the previous final result and the previous intermediate result;

determining a modular reduction of the updated final result based on the updated final result, the negative multiplicative inverse of the modulus, and the second constant;

determining a revised updated final result based on the updated final result, the modular reduction of the final result, the modulus, and the second constant;

if all digits of the plurality of digits have not been evaluated, specifying the revised updated final result as the previous final result; and

if all digits of the plurality of digits have been evaluated, specifying the revised updated final result as the final result;

determining an updated intermediate result based on the previous intermediate result;

determining a modular reduction of the updated intermediate result based on the updated intermediate result, the negative multiplicative inverse of the modulus, and the second constant;

determining a revised updated intermediate result based on the updated intermediate result, the modular reduction of the updated intermediate result, the modulus, and the first constant; and

specifying the revised updated intermediate result as the previous intermediate result.

16. The method of Claim 1, wherein the modular operation is a modular exponentiation that is based on at least the second operand (Y), a second constant (W), the modulus (M), a negative multiplicative inverse of the modulus (M′), and the intermediate result (S), wherein the second operand (Y) includes a plurality of digits, and wherein the final result (F) is determined based on the following expressions:

F = 1;

for each digit of the plurality of digits included in the second operand (Y), evaluating the following expressions:

when each digit of the plurality of digits has a value of one, then evaluating the following expressions:

$Z = SF$;

$U = ZM'(\text{mod}(W))$; and

$F = (Z + UM)/W$;

$Z = SS$;

$U = ZM'(\text{mod}(W))$; and

$S = (Z + UM)/W$.

17. The method of Claim 1, further comprising the computer-implemented steps of:

generating a plurality of residual number system (RNS) representations, wherein the plurality of RNS representations includes at least one RNS representation for each of the first operand, the modulus, and the first constant;

wherein the step of determining the intermediate result includes the computer-implemented step generating the intermediate result based on Montgomery's method for the modular operation and the plurality of RNS representations; and

wherein the step of determining the final result includes the computer-implemented step of generating the final result based on Montgomery's method for the modular operation and the plurality of RNS representations.

18. The method of Claim 17, wherein the plurality of RNS representations includes a first set of RNS representations in a first RNS base and a second set of RNS representations in a second RNS base.

19. The method of Claim 18, further comprising the computer-implemented step of:

converting a first RNS representation of the first set of RNS representations in the first RNS base to a second RNS representation of the second set of RNS representations in the second RNS base.

20. The method of Claim 18, wherein the first RNS base extends the second RNS base.

21. The method of Claim 19, wherein the step of converting is performed in eight clock cycles.

22. The method of Claim 18, wherein the first RNS base includes a first group of sixty-four residues and the second RNS base includes a second group of sixty-four residues.

23. The method of Claim 22, further comprising the computer-implemented steps of:

performing operations involving each residue in the first group in parallel; and

performing operations involving each residue in the second group in parallel.

24. The method of Claim 22, wherein each residue in both the first group and second group is a seventeen-bit residue.

25. The method of Claim 22, wherein each residue in the first group is relatively prime with respect to all other residues in the first group and each residue in the second group are relatively prime with respect to all other residues in the second group.

26. The method of Claim 22, wherein each residue in both the first group and the second group are a selected from a range of 2^{16} to 2^{17}.

27. The method of Claim 1, wherein the modular operation is a modular multiplication and the step of generating the second electronic message further includes the computer-implemented step of:

while determining the intermediate result and determining the final result, storing results of intermediate computations in a first register file and a second register file.

28. The method of Claim 27, wherein the first register file includes a first set of sixty-four seventeen-bit registers and the second register file includes a second set of sixty-four seventeen-bit registers.

29. The method of Claim 1, wherein the modular operation is a modular exponentiation and the step of generating the second electronic message further includes the computer-implemented step of:

while determining the intermediate result and determining the final result, storing results of intermediate computations, in a first register file a second register file, a third register file, and a fourth register file.

30. The method of Claim 29, wherein the first register file includes a first set of sixty-four seventeen-bit registers, the second register file includes a second set of sixty-four seventeen-bit registers, the third register file includes a third set of sixty-four seventeen-bit registers, and the fourth register file includes a fourth set of sixty-four seventeen-bit registers.

31. The method of Claim 1, wherein the steps of determining the intermediate result and determining the final result use an array of sixty-four seventeen-bit by seventeen-bit modular multiplier circuits.

32. The method of Claim 31, wherein the array of sixty-four seventeen-bit by seventeen-bit modular multiplier circuits includes a plurality of ratio four to two compressors that are organized into three levels and that are executed in one clock cycle.

33. The method of Claim 1, wherein the steps of determining the intermediate result and determining the final result use an array of sixty-four thirty-four-bit to seventeen-bit modular reduction circuits that are executed in one clock cycle.

34. A computer-readable medium carrying one or more sequences of instructions for encryption and decryption of electronic messages based on an encryption protocol, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

receiving a first electronic message that is encrypted according to the encryption protocol;

generating at least one part of a second electronic message, based on at least the first electronic message, a modular operation that is based on two applications of Montgomery's method, a first operand, a second operand, and a modulus, and wherein the instructions for generating the second electronic message further comprise instructions which, when executed by one or more processors, cause the one or more processors to carry out the steps of:

generating a first constant based on the modulus;

determining an intermediate result based on at least Montgomery's method for the modular operation, the first operand, and the first constant; and

determining and storing in memory a final result that comprises the at least one part of the second electronic message, based on at least

Montgomery's method for the modular operation, the intermediate result, and the second operand.

35. An apparatus for encryption and decryption of electronic messages based on an encryption protocol, comprising:

means for receiving a first electronic message that is encrypted according to the encryption protocol;

means for generating at least one part of a second electronic message, based on at least the first electronic message, a modular operation that is based on two applications of Montgomery's method, a first operand, a second operand, and a modulus, and wherein the means for generating the second electronic message further comprises:

means for generating a first constant based on the modulus;

means for determining an intermediate result based on at least Montgomery's method for the modular operation, the first operand, and the first constant; and

means for determining and storing in memory a final result that comprises the at least one part of the second electronic message, based on at least Montgomery's method for the modular operation, the intermediate result, and the second operand.

36. An apparatus for encryption and decryption of electronic messages based on an encryption protocol, comprising:

an interface;

a processor coupled to the interface and receiving information from the interface; and

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

receiving a first electronic message that is encrypted according to the encryption protocol;

generating at least one part of a second electronic message, based on at least the first electronic message, a modular operation that is based on two applications of Montgomery's method, a first operand, a second operand, and a modulus, and wherein the instructions for generating the second electronic message further comprise instructions which, when executed by the processors, cause the processor to carry out the steps of:

generating a first constant based on the modulus;

determining an intermediate result based on at least Montgomery's method for the modular operation, the first operand, and the first constant; and

determining and storing in memory a final result that comprises the at least one part of the second electronic message, based on at least Montgomery's method for the modular operation, the intermediate result, and the second operand.